REMARKS

The present Amendment is responsive to the Official Action of January 16, 2007 and is filed concurrently with a request for continued examination. In the Official Action, Claims 1-5 were rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6,412,069 to Kavsan ("*Kavsan*") in view of the non-patent reference "F-Secure Kernel Mode Cryptographic Driver (Microsoft Windows NT/2000/XP) FIPS 140-2 Validation Security Policy, Created: December 2001, Module Version: 1.1, by Alexey Kirichenko ("*Kirichenko*"). Claims 6-7 were rejected under 35 U.S.C. § 103(a) as being obvious over *Kavsan* in view of both *Kirichenko* and U.S. Published Patent Application No. 2004/0078568 to Pham *et al.* ("*Pham*"). Claims 8-21 were rejected under 35 U.S.C. § 103(a) as being obvious over International Published Patent Application No. WO 01/80482 to Eun *et al.* ("*Eun*") in view of *Kirichenko*. Claims 22-29 were rejected under 35 U.S.C. § 103(a) as being obvious over *Eun* in view of *Pham*.

By this Amendment, Claim 18 has been amended. Also, the specification has been amended to correct typographical errors. Reconsideration of the claims in view of the preceding amendments and the following remarks is respectfully requested.

I. Rejection of Claim 1

Independent Claim 1 is directed to a method for protecting an operating system, comprising, "determining integrity data for an operating system binary, wherein the integrity data enables detection of a modification to the operating system binary; and modifying a kernel with the integrity data, wherein the kernel is operable to employ the integrity data to detect the modification to the operating system binary."

Claim 1 was rejected over the combination of *Kavsan* and *Kirichenko*. *Kavsan* discloses cryptographic (*i.e.*, encryption) service software that performs cryptographic services in the kernel space of an operating system. *See* Abstract of *Kavsan*. *Kirichenko* discloses a cryptographic module that runs as a kernel mode software module (*i.e.*, in the kernel space). *See Kirichenko*, p. 3.

The Official Action admits that *Kavsan* does not explicitly disclose determining integrity data and detection of a modification to an operating system binary, as recited by Claim 1. *See* p. 5 of the Official Action. However, the Official Action indicates that this deficiency is cured by the disclosure at p. 7, paragraph 3 of *Kirichenko*. The cited portion of *Kirichenko* discloses a cryptographic module that runs in kernel mode and is capable of performing an integrity test on itself upon installation. *Kirichenko* describes this self test process at p. 7, paragraph 3, stating that

> When the OS loader attempts to load the Module into memory, the Module runs an integrity test and a number of cryptographic functionality self-tests. If all the tests pass successfully, the Module makes a transition to "User Service" state, where the API calls can be used by other kernel mode drivers to obtain desired cryptographic services. Otherwise, the Module returns to "Uninitialized" state and the OS reports failure of the attempt to load it into memory.

This self test appears to be entirely contained within the cryptographic module (the "Module"). Therefore, the self test cannot involve integrity data that both is determined for an OS binary and modifies a kernel as required by Claim 1, as the test only involves data regarding the Module.

For at least the above reasons, Applicants respectfully submit that Claim 1, and each of the claims depending therefrom, is patentable over *Kavsan* and *Kirichenko*, taken either individually or in combination.

II. Rejection of Claims 8 and 18

Independent Claim 8 is directed to a method for protecting an operating system, comprising, *inter alia*, "performing a tamper detection action if the first integrity data indicates tampering of the operating system binary." Independent Claim 18 is directed to a method for protecting an operating system, comprising, *inter alia*, "performing a tamper detection action if the integrity data indicates tampering of the operating system binary." Both of these claims were rejected over the combination of *Eun* and *Kirichenko*.

Eun is directed to a method and apparatus for protecting a file system. *See Eun*, Abstract. In general, *Eun* discloses the use of a digital signature-based authentication process in which a user seeking access to a computer file system is identified through a digital signature to determine whether the user is authorized for the sought access. *See, e.g.*, p. 2, ll. 14-28 of *Eun*. As mentioned earlier, *Kirichenko* discloses a cryptographic module that runs as a kernel mode driver and performs a self test.

Neither *Eun* nor *Kirichenko* appears to disclose at least performing a tamper detection action when integrity data indicates tampering of the operating system binary, as recited in one form or another in Claims 8 and 18. The digital signature-based authentication of *Eun* and the data encryption of *Kirichenko* are unrelated to the determining of tampering, and, as such, do not involve "integrity data," which is described in the specification of the present application as data that enables detection of a modification to the OS binary. *See, e.g.*, ¶¶ 0006 and 0007 of the present application. Further, as stated earlier, the self test of *Kirichenko* appears to be entirely contained within the cryptographic module, and therefore cannot involve integrity data that is for an OS binary but incorporated into (and retrievable from) a kernel.

The Official Action cites *Eun* p. 5, ll. 11-20 and 28-34, and also p. 6, ll. 4-11, as disclosing "generating a first integrity data associated with an operating system binary;" and further cites Fig. 3 as disclosing "performing a tamper detection action if the first integrity data indicates tampering of the operating system binary." *See* pp. 8, 9, and 12 of the Official Action. However, these portions of *Eun* describe the process for verifying a digital signature using encryption keys. Such operations for assessing affirmative indications of identity or authority are quite different from techniques designed to detect unannounced data modifications, as enabled by Claims 8 and 18.

For at least the above reasons, Applicants respectfully submit that Claims 8 and 18, and the claims respectively depending therefrom, are patentable over the combination of *Eun* and *Kirichenko*.

III. Rejection of Claims 22 and 29

Independent Claim 22 is directed to a computer-readable medium having computer-executable components for protecting an operating system, comprising, *inter alia*, "a data store configured to receive and store a first integrity data, wherein the first integrity data is for an operating system binary; and a tamper detection component, coupled to the data store, that is arranged to perform actions, including . . . determining if the first integrity data indicates tampering of the operating system binary . . ." Independent Claim 29 is directed to an apparatus for protecting an operating system, comprising, *inter alia*, "means for retrieving a first integrity data for the operating system binary; means for determining a second integrity data for the operating system binary; and means for determining if the first integrity data is substantially different from the second integrity data, and if the first integrity data is substantially different from the second integrity data, a means for performing a tamper detection action." These claims were rejected as being obvious over the combination of *Eun* and *Pham*.

As indicated above, *Eun* discloses the use of a digital signature-based authentication process in which a user seeking access to a computer file system is identified through a digital signature to determine whether the user is authorized for the sought access. *Pham* discloses providing a security file system layer that is structured to implement a file access control function that selectively constrains data transfer operations initiated through the operating system kernel by an application program to transfer file data through the file system with respect to a persistent data store. A file access controller, implemented independent of the operating system kernel, is coupled to the security file system layer and supports the file access control function by defining permitted file data transfers through the file system. *See* ¶ 0013 of *Pham*.

The Official Action admits that *Eun* fails to disclose "performing a tamper detection action [for an operating system binary]." *See* pp. 14 and 16 of the Official Action. The Official Action then cites Figs. 10B and 12B of *Pham* as disclosing this subject matter. However, as described above, all of *Pham*, including the cited figures, discloses a process in which

authentication is performed for user applications. *Pham* does not disclose the use of integrity data for authenticating or detecting tampering of an OS binary.

For at least the above reasons, Applicants respectfully submit that independent Claims 22 and 29, as well as the claims respectively depending therefrom, are patentable over the combination of *Eun* and *Pham*.

CONCLUSION

In view of the amended claims and the foregoing remarks, it is respectfully submitted that all of the claims of the present application are in condition for immediate allowance. It is therefore respectfully requested that a Notice of Allowance be issued. The Examiner is encouraged to contact Applicant's undersigned attorney to resolve any remaining issues in order to expedite examination of the present application.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.

Respectfully submitted,

/Richard D. Emery/

Richard D. Emery
Registration No. 58,894

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111
LEGAL02/30444996v1